Building Secure Systems Using Model-Based Engineering and Architectural Models

Dr. Jörgen Hansson, Dr. Peter H. Feiler, and John Morley. The Department of Defense's policy of multi-level security (MLS) has long employed the Bell-LaPadula and Biba approaches for confidentiality and integrity; more recently, the multiple independent levels of security/safety (MILS) approach has been proposed. These approaches allow designers of software-intensive systems to specify security levels and requirements for access to protected data, but they do not enable them to predict runtime behavior. In this article, model-based engineering (MBE) and architectural modeling are shown to be a platform for multi-dimensional, multi-fidelity analysis that is conducive for use with Bell-LaPadula, Biba, and MILS approaches, and enables a system designer to exercise various architectural design options for confidentiality and data integrity prior to system realization. In that way, MBE and architectural modeling can be efficiently used to validate the security of system architectures and, thus, gain confidence in the system design.

Back[1]

Part "Attachment Data"

Mime-type: application/pdf, size: 154050 bytes

[1] https://buildsecurityin.us-cert.gov/adm-bsi/1185-BSI.html